METHOD FOR ACCESSING A DATA PROCESSING SYSTEM

BACKGROUND

[0001] The invention relates to a method for accessing a data processing system.

[0002] According to the prior art, data processing systems which are composed of a multiplicity of data processing units, for example personal computers, computer-controlled equipment, servers and the like which are networked to one another for the exchange of data, are widely known. In this context, each data processing unit is assigned a restricted number of users. In order to prevent unauthorized use of a data processing unit, each user has a personal password. By inputting the password the user proves his authentication and receives access to the data processing system.

[0003] In particular in hospitals, data processing systems are complex nowadays. Inter alia, diagnostic and analytical devices are components of such data processing systems. Such devices must always be kept in a satisfactory functional state. In particular, maintenance and repair of such devices generally requires access via a system technician to the data processing system. A problem which continues to be unresolved is that the system technician therefore can under certain circumstances receive access to personal patient data. For reasons of data protection law, such a data processing system can be accessed only according to the two man principle, i.e. only by two authorized persons at the same time. In practice, this is however virtually impossible to implement because if there is a functional fault in a data processing system immediate remedy is generally necessary and in some cases two authorized system technicians which are sufficiently qualified to deal with the functional fault are not always available at the same time.

[0004] **DE 101 21 819 A1** discloses a method in which a doctor is provided with access to patient-specific data only if the doctor reads in a first chip card assigned to him and the patient, who is present at the same time, reads in a second

chip card, which belongs to him, into the data processing device at the doctor's surgery (station), for the purpose of authentication.

[0005] The object of the invention is to specify a method which permits access, which ensures control over the data by a system administrator, to a data processing system only according to the two man principle.

[0006] This object is achieved by means of the features of claim 1. Expedient refinements of the method result from the features of claims 2 to 13.

[0007] According to the invention, a method for accessing a data processing system, which is formed from data processing units which are networked to one another for the exchange of data, is provided, having the following steps:
providing a first authentication means (9) for authenticating a system administrator, authenticating the system administrator on a first data processing unit by transferring the first authentication means to an authentication program, providing a second authentication means for authenticating a system technician, authenticating the system technician on a second data processing unit by transferring the second authentication means to the authentication program and resulting automatic generation of an identification information item which identifies the carrier of the second authentication means, displaying the identification information item on the first data processing unit (1) of the system administrator and enabling access authorization for the system technician and automatic triggering of a function for generating and storing a log file which logs the activity of the system technician on the data processing system.

[0008] According to the inventive method

[0009] The system technician is not provided with access to the data processing system until after a second authentication means which that is assigned to him has been transferred. The enabling of such access is documented by the generation of an identification information item and is displayed on the first data processing unit of the system administrator. A log file thatwhich logs the activity of the system technician and by reference to which the intervention by the system technician can be tracked, for example by the system administrator, is also generated. This ensures that the system administrator always has control over the

data. By means of tThe generated log files make it is possible for him to check whether a system technician has access to data without authorization. In this case, the system administrator can immediately block any further access to the data processing system for the respective system technician. With the proposed method,Thus, access to a data processing system is made possible according to the two man principle. Here, it is of particular It is advantagadvantageouse that such access can only take place only if the system administrator, with has knowledge of knowledge of the system administrator, only one system technician is active on one data processing unit.

[0010] The term "access" is understood in the sense of the present invention to mean any activity during which the data stock (stack) of a data processing system is inspected, changed or copied in its entirety or partially. A "data processing unit" in the sense of the present invention is a device which is connected, for the exchange of data, to other devices which are suitable for the exchange of data. For the exchange of data, such devices usually have a bidirectional interface. These devices can be a personal computer, computer-controlled systems or devices or the like.

[0011] The term "system administrator" is understood to refer to a person who has particular rights with respect to the management and maintenance of the data processing system. In contrast to a system technician, the system administrator in the sense of the present invention is able to permit or block access to the data processing system. This possibility is assigned to the system administrator in particular by means of the first authentication means. Inauthentication.

[0012] In order to authenticate the system technician, the second authentication means can be compared by means of the authentication program by accessing a file containing averified, second authentication means, and when there is correspondence with one of the verified, second authentication means a corresponding information item is transferred to the system administrator. A "verified, second authentication means" is understood to be a copy of the second authentication means which that has been transferred to the system technician. and saidThis copy is managed by the system administrator in a file which only he

can access. In order to access the data processing system, the system administrator transfers a particular, second authentication means to each system technician. In order to facilitate the checking of the authenticity of the second authentication means, these are stored together in the file. If the authentication program detects that an access request is present on the basis of a second authentication means which is identical to a verified, second authentication means, this is indicated to the system administrator by means of a suitable information item. Each verified, second authentication means contained in the file is advantageously assigned an identification information item which is specific thereto. This information item can be, for example, the name and, if appropriate, the membership of the system technician of a specific organization. If the second authentication means corresponds to a verified, second authentication means which is stored in the file, the name and the organization of the system technician can therefore be additionally displayed to the system administrator.

[0013] In a particularly simple case, the first and/or second authentication means are an authentication code which can be transferred to the authentication program preferably by means of a keypad which is provided on a data processing unit. In order to increase security it is expedient for the authentication code to be stored in a mobile memory unit which can be connected to the data processing system for the transmission of data. The memory unit may be an authentication card which is provided with a data carrier. The authentication card can have a memory means, in particular for storing the log file, and/or an information item which permits access to the log file. The information item can be, for example, a"link" which can be used to locate and open the log file.

[0014] In order to increase the security, the enabling of an access authorization is done via the system administrator by manually triggering a function which is provided for this purpose in the authentication program, and can be accessed exclusively by the system administrator. This ensures that access occurs only with the active consent of the system administrator. However, it may also be the case that access is automatically granted to the system technician after automatic checking of the second authentication means. In this case also, in particular a log

file is produced automatically according to the invention. This permits access to data processing systems, in particular in hospitals, which have to be kept functionally available without interruption.

[0015] According to a further refinement, provision is made for the connection between the first data processing unit and the second data processing unit to be established via the Internet or via an intranet. This permits access by the system technician from a remote location, second data processing unit. It is thus possible for a system technician who has optimum qualifications for the respective problem to access the data processing system at any time, i.e. irrespective of his location. This permits rapid and effective elimination of functional faults. At the same time, in this context the authenticity of the accessing system technician is ensured and his activity is logged. The access by the system technician also takes place in this case according to the two man principle. By means of the data processing system it is possible, in particular, to process data which an individual person can access only with particular authorization, or only by persons with a simple authorization according to the two man principle when the particular authorization is not present. Proof of the particular authorization is expediently given by transferring a third authentication means, assigned to the person, to the data processing system. The individual person with particular authorization may be, for example, a doctor. The data may be personal data which requires protection, in particular patient data.

drawings

[0016] exemplary embodiment of the invention will be explained in more detail below with reference to the drawing, in which:

[0017] fig. 1 shows the method by means of a schematic overview, and

[0018] fig. 2 shows the essential features of an authentication program.

DETAILED DESCRIPTION OF THE DRAWINGS AND THE PRESENTLY PREFERRED EMBODIMENTS

[0019] Fig. 1 is a schematic view of a first data processing unit 1, for example a personal computer. The first data processing unit 1 is a component of a first networked data processing system D1 which comprises, as further data processing

units, for example, computer-controlled devices 2 or further personal computers 3. The first data processing unit 1 is assigned to a system administrator 4 who has data control over the first data processing unit D1. The system administrator 4 is authorized in particular to assign roles and rights to users of the first data processing system D1 by means of a first program 5. Such roles and rights permit the respective user only to have access to the data which is necessary for his area of work. The users can access such data at any time, i.e. even if the system administrator 4 is not logged into the first data processing system D1.

[0020] The first data processing system D1 is logged into a second data processing system D2 of a service organization via a data line which is protected with a firewall 6. The connection can be established, for example, via the Internet or an intranet. The second data processing system D2 comprises a second data processing unit 7, for example a personal computer, which is assigned to a system technician 8.

[0021] The system administrator 4 has, for its authentication, a first memory card 9 on which a first authentication code is stored. The first authentication code can be made available for reading out by means of a suitable reading device of the first data processing system D1. The system technician 8 has, for his authentication, a second memory card 10 on which a second authentication code is stored. The second authentication code can be read out and the first data processing system D1 can be allowed to access it by means of a suitable reading device. The reading unit for reading out the second memory card 10 does not necessarily need to be a component of the first data processing system D1 here. It can also be a component of the second data processing system D2. In this case, the authenticity of the second authentication code can be checked by means of a second program 11, provided in the second data processing system D2, before an attempt is made to access the first data processing system D1.

[0022] The function of the device is as follows:

[0023] At first, an IT manager 12 who is responsible for the first data processing system D1 and a service organization or the system technician 8 conclude a service contract. After such a service contract has been concluded, the

system technician 8 receives, from the IT manager 12, a second memory card 10 on which the second authentication code is stored.

[0024] In a first maintenance/repair situation, the system administrator 4 requests a service from the service technician 8 by means of a telephone call or by e-mail. This may be a service which can be performed from the second data processing unit 7. In this case, the service technician 8 transfers the second memory card 10 to a reading device which is provided at the second data processing unit 7. As a result, the second authentication code which authenticates the service technician 8 within the second data processing system D2 is transferred to the second program 11. The second authentication code is checked. If the second program 11 recognizes the second authentication code as authentic, a connection is established to the first data processing system D1 via the data line. The desired access is checked by means of the first program 5. For this purpose it is initially checked whether the first memory card 9 is inserted into a reading device, for example at the first data processing unit 1. If this is not the case, access by the system technician 8 is not allowed. If access to the first authentication code which is stored on the first memory card 9 is possible in order to authenticate the system administrator 4, the second authentication code is compared with a multiplicity of second authentication codes which are stored in a file. If the second authentication code is recognized as not being authentic, access by the system technician 8 is not allowed. If the second authentication code is recognized as being authentic, a log function is triggered. At the same time, the system technician 8 is provided with access to the first data processing system D1. As long as the service technician 8 accesses the first data processing system D1, all the changes, supplements and the like to the data stock (stack) of the first data processing system D1 are logged. As soon as the system technician 8 has concluded his activity and has logged off, the log file is closed.

[0025] The log file advantageously contains both the log of all the changes, supplements and the like to the data stock (stack) of the first data processing system D1 and in addition the following information: name of the system

technician, name of the service organization, login/Logout time, and method of access, if appropriate identification of the data processing unit used for access.

[0026] In a second maintenance/repair situation, the system administrator requests a service - which is to be carried out in situ - from the service technician 8 by means of a telephone call or by e-mail. The service may comprise, for example, exchanging a module on an X-ray computed tomograph in a hospital. In this case, the service technician 8 logs in on a suitable data processing unit of the first data processing system D1 using the second memory card 10. In this case also, access is possible only if the system administrator 4 is logged into the first data processing system D1 at the same time using the first memory card 9.

[0027] According to a further advantageous function, the system administrator 4 can interrupt the activity of the system technician 8 at any time by interrupting access to the first data processing system D1 by interrupting the access to the first authentication code. This may be done, for example, by the system administrator 4 removing the first memory card 9 from the respective reading device. In contrast to conventional methods, with the method according to the invention the system administrator 4 always keeps control over the data. Furthermore, by using the automatic logging function it is possible to track all the activities of the system technician 8. In the case of misuse it is possible to readily block a further access by the system administrator 8 to the first data processing system D1. To do this, the respective second authentication code which is stored in the file must merely be removed or changed.

[0028] With the proposed method, access by the system technician 8 to the data stock (stack) of the first data processing system D1 is possible only according to the two man principle, i.e. such access always occurs under the control of the system administrator 4. To this extent, unauthorized access by the system technician 8 to personal data which requires protection, for example patient data, can always be prevented.

[0029] **Fig. 2** is a schematic view of the essential components of the first program 5. UI1 is a first user interface for access by the first data processing

system D1 and UI2 is a second user interface for access, for example, via the data line.

[0030] An access module 13 permits or blocks access for a system technician 8 to the first data processing system D1. The access module 13 manages and compares, in particular, authentication codes.

[0031] The first program 5 can advantageously have further modules which facilitate, in particular, maintenance and/or repair work on the first data processing system D1. It is thus possible, for example, for a localization module 14 to be provided with which it is possible to detect at which data processing unit a qualified system technician 8 is currently active, and at which he can be called if necessary.

[0032] The logging module 15 brings about logging of the activity of the system technician 8. With the logging module 15, in particular log files are produced and stored at a predefined location.

[0033] An anonymization module 16 serves, in particular, to anonymize personal data which requires protection. For example, it is possible to replace names of patients by codes so that, in accordance with the data protection regulations, a system technician 8 is prevented from viewing personal data.

[0034] Auxiliary modules 17, 18 make available a description of the functions of the first program 5 which are necessary for the system administrator 4 and the system technician 8. A modality module 19 permits data to be exchanged, for example with computer-controlled devices such as X-ray computed tomographs etc. In a similar way, an IT system module 20 permits data to be exchanged with databases etc.

[0035] An operating system module 21 provides the necessary conditions for correct integration of the first program 5 into the respectively used operating system.